M.H

RÉPUBLIQUE FRANÇAISE

INPI INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

EJU

FR99/1996

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 20 AOUT 1999

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

SIEGE
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
26 bis, rue de Saint Petersbourg
75800 PARIS Cédex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : (1) 42.94.52.52 Télécopie : (1) 42.93.59.30

BREVET D'INVENTION, CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle-Livre VI

cerfa N° 55-1328

REQUÊTE EN DÉLIVRANCE

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES : 17 AOUT 1998
N° D'ENREGISTREMENT NATIONAL : 98 10592
DÉPARTEMENT DE DÉPÔT : 75
DATE DE DÉPÔT : 17 AOUT 1998

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

NONNENMACHER BERNARD
GEMPLUS SCA
PARC D'ACTIVITE DE GENENOS
AVENUE DU PIC DE BERTAGNE
13420 GENENOS
n° du pouvoir permanent : références du correspondant : GEM 576 téléphone :

2 DEMANDE Nature du titre de propriété industrielle

☐ brevet d'invention ☐ demande divisionnaire ☐ demande initiale
☐ certificat d'utilité ☐ transformation d'une demande de brevet européen ☐ brevet d'invention ☐ certificat d'utilité n° date

Établissement du rapport de recherche ☐ différé ☒ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance ☐ oui ☒ non

Titre de l'invention (200 caractères maximum)

PROCEDE DE TEST DE SOURCE DE NOMBRE ALEATOIRE ET DISPOSITIFS ELECTRONIQUES COMPRENANT CE PROCEDE

3 DEMANDEUR (S) n° SIREN 349711200 code APE-NAF

Nom et prénoms (souligner le nom patronymique) ou dénomination : GEMPLUS

Forme juridique : S.C.A

Nationalité (s) : FRANCAISE

Adresse (s) complète (s) : PARC D'ACTIVITE DE GENENOS
AVENUE DU PIC DE BERTAGNE
13420 GENENOS

Pays : FRANCE

En cas d'insuffisance de place, poursuivre sur papier libre ☐

4 INVENTEUR (S) Les inventeurs sont les demandeurs ☐ oui ☒ non Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES ☐ requise pour la 1ère fois ☐ requise antérieurement au dépôt ; joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine	numéro	date de dépôt	nature de la demande

7 DIVISIONS antérieures à la présente demande n° date n° date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (nom et qualité du signataire - n° d'inscription)

NONNENMACHER BERNARD
DIRECTEUR PROPRIETE INDUSTRIELLE

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION | SIGNATURE APRES ENREGISTREMENT DE LA DEMANDE À L'INPI

La loi n°78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION, CERTIFICAT D'UTILITE

DÉSIGNATION DE L'INVENTEUR
(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

DIVISION ADMINISTRATIVE DES BREVETS
26bis, rue de Saint-Petersbourg
75800 Paris Cédex 08
Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30

N° D'ENREGISTREMENT NATIONAL

9810592

TITRE DE L'INVENTION :

PROCEDE DE TEST DE SOURCE DE NOMBRE ALEATOIRE ET DISPOSITIFS ELECTRONIQUES COMPRENANT CE PROCEDE

LE(S) SOUSSIGNÉ(S)

GEMPLUS

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

JEAN-SEBASTIEN CORON
4 RUE LEON DE LAGRANGE
75015 PARIS

DAVID NACCACHE
7 RUE CHAPTAL
75009 PARIS

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

13/08/98

BERNARD MONNEMACHER
DIRECTEUR PROPRIETE INDUSTRIELLE

RA 1132771196

PROCEDE DE TEST DE SOURCE DE NOMBRE ALEATOIRE ET DISPOSITIFS ELECTRONIQUES METTANT EN OEUVRE CE PROCEDE

L'invention concerne un procédé de test de sources générant des nombres aléatoires, en particulier des sources mises au point dans le cadre de systèmes cryptographiques tels que les générateurs de nombres aléatoires embarqués à bord de cartes à puce.

Elle est particulièrement destinée à être mise en oeuvre dans le test et la validation de dispositifs électroniques du type carte à puce, PCMCIA, badges, cartes sans contact ou tout autre appareil portable.

La plupart des systèmes de cryptographie à clé publique (dite aussi cryptographie asymétrique) et clé secrète (dite aussi cryptographie symétrique) nécessitent le tirage d'aléas secrets. Il est primordial que de tels aléas, ou nombres, destinés à servir comme clés ultérieurement , soient à priori imprévisibles et ne présentent pas de régularités permettant de les retrouver par des stratégies de recherche exhaustive ou exhaustive améliorée pour laquelle les clés les plus probables sont cherchées en premier lieu.

A ce titre, il existe plusieurs procédés permettant de tester les aléas générés par une source aléatoire et de s'assurer que ladite source fonctionne correctement et ne présente pas de dérive suite à des changements de paramètres externes d'origine malveillante telle qu'une altération par des radiations induites.

Chacun de ces procédés s 'applique à une suite, appelée aussi séquence, de nombres entiers compris entre 0 et une valeur d, ladite suite étant générée par la source aléatoire.

Le procédé de test le plus connu est le test dit de "fréquence". Il s'agit de compter le nombre d'apparitions de chaque entier compris entre 0 et une valeur d dans ladite séquence. Le nombre d'apparitions de chaque entier est ensuite évalué statistiquement.

Un second procédé de test dit de "séries" consiste en un comptage et une évaluation statistique du nombre d'apparitions de tous les couples possibles d'entiers compris entre 0 et une valeur d. Ce

procédé de test peut être généralisé au comptage des triplets, quadruplets d'entiers, etc...

Un troisième procédé de test dit de "trou" existe. Un trou dans une séquence est une suite de nombres à l'extérieur d'un intervalle prédéterminé. Il s'agit d'une évaluation statistique de la longueur desdits trous dans la séquence.

Un quatrième procédé de test, dit test du "poker", existe. Le test consiste à grouper les nombres de la séquence par groupe de cinq nombres et à compter dans chaque quintuplet combien de valeurs différentes apparaissent.

Un cinquième procédé de test dit de "collecte de coupons" consiste à évaluer statistiquement la taille de séquence nécessaire pour que toutes les valeurs entières comprises entre 0 et d apparaissent dans ladite séquence.

Le détail de ces procédés se trouve dans l'ouvrage intitulé: " Knuth, The art of computer programming, vol. 2, Seminumerical algorithms ".

Un autre procédé de test populaire est le test universel de Maurer décrit dans l'ouvrage " Journal of Cryptology, vol. 5, n° 2, 1992, pp. 89-105 ". Ce test présente l'avantage de révéler tous les défauts décelables par les procédés de tests précédemment cités ainsi que d'autres défauts statistiques non détectés par ces mêmes procédés de test.

Le procédé de test, dit de Maurer, également dénommé universel, comprend les étapes suivantes:

Première étape: Génération d'une séquence de (Q+K)*L bits par la source aléatoire. Q, K et L sont des paramètres d'entrée. Les bits de la séquence sont groupés par bloc de L bits, formant une séquence d'entiers compris entre 0 et 2^L-1 de longueur Q+K. La longueur est mémorisée dans le tableau block[n], où n est compris entre 1 et Q+K.

Deuxième étape: Calcul du paramètre du test, noté fTU; cette deuxième étape comprenant les étapes suivantes, appelées sous-étapes 2.1 à 2.5 :

2.1 Création et initialisation d'un tableau tab [i] de taille 2^L;

2.2 Pour n variant de 1 à Q, faire le calcul: tab[block[n]]=n;

2.3 Initialiser le nombre Sum à 0;

2.4 Pour n variant de Q+1 à Q+K, exécuter le calcul :

Ajouter log(n-tab[block[n]] à Sum;

Faire le calcul: tab[block[n]]=n;

2.5 Le paramètre fTU du test est donné par:

fTU=(Sum/K)/Log(2);

Troisième étape: Calcul de la variance par block de paramètre du test, notée Var. Son expression précise est donnée dans l'article publié par Maurer dans l'ouvrage " Journal of Cryptology, vol. 5, n° 2, 1992, pp. 89-105 ", qui est :

$$Var= (1-z)^* \sum_{i=1}^{\infty} \log2(i)^2 * z^{i-1} - ((1-z)^* \sum_{i=1}^{\infty} \log2(i)^* z^{i-1})^2 ,$$

avec log2(z)=log(z)/log(2) et $z=1-2^{-L}$

Quatrième étape: Calcul de la fonction c(L,K). Une expression approchée de cette fonction est donnée dans l'article de l'ouvrage précédent, qui est:

c(L,K)=0,7-0,8/L+(1,6+12,8/L)*K(-4/L);

Cinquième étape: Calcul de l'écart type du paramètre de test, noté σ: $\sigma=c(L,K)^*\sqrt{(Var/K)}$;

Sixième étape: Calcul du paramètre y; y est déterminé à partir du taux de rejet du test fixé en entrée, noté ρ. y doit vérifier l'équation:

$N(-y)= \rho$.

N est la fonction de densité normale décrite dans l'ouvrage " R. Langley, Practical statistics, Dover publications, New-York, 1968 ".

L'équation $N(-y)= \rho$ peut être résolue en utilisant une table de valeurs de N. Une telle table est fournie dans l'article précédent;

Septième étape: Calcul de la valeur moyenne idéale du test, notée E[fTU]. Son expression est donnée dans l'article publié par Maurer dans l'ouvrage " Journal of Cryptology, vol. 5, n°2, 1992, pp. 89-105 ", et vaut :

$$E[fTU]= (1-z)^* \sum_{i=1}^{\infty} \log2(i)^* z^{i-1}$$

avec log2(z)=log(z)/log(2) et $z=1-2^{-L}$

Huitième étape: Calcul des bornes t1 et t2. Elles sont données par l'équation: $t1=E[fTU]-y^*\sigma$ et $t2=E[fTU]+y^*\sigma$;

Neuvième étape: Résultat du test:

Si le paramètre du test fTU est compris entre t1 et t2, alors le générateur de nombre aléatoire est accepté. Dans le cas contraire, il est refusé.

Le procédé de test universel est donc basé sur une approximation dans le calcul de la fonction c(L,K). Cette approximation rend le test moins précis que ce que veut la garantie théorique lui servant de base. Il est possible de montrer que dans certains cas, le test universel s'avère 2,67 fois trop permissif par rapport à ce que permet la théorie.

La présente invention a pour objet un procédé de test amélioré permettant d'atteindre la précision réelle garantie par l'analyse théorique du test universel. Ce test sert notamment à améliorer la sécurité de dispositifs portables du type carte à puce.

Le procédé de l'invention consiste à remplacer l'étape 4 du test universel par le calcul précis de la fonction c(L,K). Ce calcul est basé sur une analyse probabiliste du test universel.

La présente invention donne trois expressions distinctes de la fonction c(L,K), suivant les valeurs des paramètres L et K.

La première expression de c(L,K) est valable quelque soient les paramètres L et K.

La deuxième expression de c(L,K) est valable dans le cas où la valeur L est comprise entre 3 et 16 et la valeur K est supérieur à 30^*2^L, ce qui correspond au cas le plus usuel d'utilisation du test. Elle est beaucoup plus simple à calculer que la première expression et peut donc s'effectuer à bord d'un simple micro-controleur en quelques millisecondes.

La troisième expression de c(L,K) est valable pour une valeur de $L>16$ et une valeur de $K>30^*2^L$.Cette expression est encore plus simple à calculer.

La première expression de c(L.K) peut s'obtenir par le procédé décrit ci-dessous qui comporte neuf étapes:

1. Calculs de: $u=1-2^{-L}$ et $v=1-1/(2^{L}-1)$;
   u et v étant des nombres réels;

2. Création de deux tableaux tab1 et tab2 de dimension $60*2^{L}$;

3. Remplissage des tab1 et tab2: pour cela,
   3.1 Exécuter z=u, sum=0, z1=1;
   3.2 Pour i allant de 1 à $30*2^{L}$, répéter les deux opérations qui sont: ajouter log2(i)*z1 à sum, dans laquelle log2 désigne le logarithme en base 2, et
   calculer: z1=z1*z;
   3.3 Exécuter tab1[0]=(1-z)*sum;
   3.4 Pour i allant de 1 à $60*2^{L}$,
   Exécuter tab1[i]=(tab1[i-1]-(1-z)*log2(i))/z;
   3.5 Répéter les étapes 3.1, 3.2, 3.3, 3.4 en remplaçant u par v et tab1 par tab2;
4. Calcul de la variance par bloc notée Var;
   4.1 Exécuter sum=0 et x=1;
   4.2 Pour i variant de 1 à $30*2^{L}$, exécuter les deux opérations qui sont:
   Ajouter $\log2(i)^{2}*x$ à sum et
   Exécuter x=x*z;
   4.3 Faire $Var=sum/2^{L}-tab1[0]^{2}$;
5. Calcul de P(K):
   5.1 Faire sum=0 et x=1
   5.2 Pour i variant de 1 à $30*2^{L}$: faire les trois opérations suivantes:
   Calculer y: $y=u^{2}*(tab2[i+K-1]-tab1[i+K])*(tab2[0]-v^{i}*tab2[i])+u*tab1[0]*(tab1[i+K-1]-tab2[i+K-1])$,
   Ajouter y*x à sum,
   Exécuter x=x*u;
   5.3 Exécuter $P(K)=u^{(K-1)}*sum$;

6. Calcul de P(1):

Même procédé qu'à l'étape 5 en remplaçant K par 1;

7. Calcul de Q(K):

7.1 Faire sum=0, sum2=0 et x=1,

7.2 Pour i variant de 1 à 30*2^L:

Ajouter $i*\log2(i)*u^{(i-2)}$ à sum2;

Exécuter les trois opérations suivantes:

calculer $y=u^{2}*(tab2[i+K-1]-tab1[i+K])*((i+k)*tab2[0]-v^{i}*tab2[i])-2^{(-L)}*sum2)+u*(i+K-1)*tab1[0]*(tab1[i+K-1]-tab2[i+K-1])$,

Ajouter y*x à sum,

Exécuter x=x*u;

7.3 Exécuter $Q(K)=u^{(K-1)}*sum$

8. Calcul de Q(1)

Même procédé qu'à l'étape 7 en remplaçant K par 1

9. Calcul de c(L,K)

$c(L,K)=\sqrt{(1-2/Var*(P(1)-P(K)-(Q(1)-Q(K))/K)}$

La deuxième expression de c(L,K) est valable pour $K>30*2^{L}$.

Elle se calcule d'après le procédé suivant en deux étapes:

Première étape: Lecture des valeurs de e(L) et d(L), e et d étant des réels, listées dans le tableau suivant, pour L compris entre 3 et 16:

L	d(L)	e(L)
3	0, 2732725	0,4890883
4	0,3045101	0,4435381
5	0,3296587	0,4137196
6	0,3489769	0,3941338
7	0,3631815	0,3813210
8	0, 3732189	0,3730195
9	0,3800637	0,3677118
10	0,3845867	0,3643695
11	0,3874942	0,3622979
12	0,3893189	0,3610336
13	0,3904405	0,3602731

14	0,3911178	0,3598216
15	0,3915202	0,3595571
16	0,3917561	0,3594040

Deuxième étape: Calcul de la valeur c(L,K) à l'aide de la formule:

$$c(L,K)=\sqrt{(d(L)+e(L)*2^{L}/K)}$$

La troisième expression de c(L,K) est valable pour L>16 et K>30*2^{L}. Elle est donnée par la formule suivante:

$$c(L,K)=\sqrt{(1-6/\Pi^{2}+2/\Pi^{2}*(4*\log(2)-1)*2^{L}/K)}$$

La présente invention concerne également, comme cela a été dit au début de la description, page une, un dispositif électronique non représenté par une figure ou un schéma. Ce dispositif électronique est un dispositif d'auto-vérification d'intégrité physique d'un circuit intégré s'auto-vérifiant et contrôlant l'intégrité de son générateur aléatoire à partir des trois variantes du procédé de l'invention, décrits également ci-dessus , ou plus explicitement à partir des trois expressions distinctes de la fonction c(L, K), ceci afin de s'assurer que ledit générateur fonctionne correctement en général et ne présente pas de dérive suite à des changements de paramètres externes d'origine malveillante telle qu'une altération par des radiations induites en particulier.

De manière préférentielle, le dispositif électronique effectuant le test est un dispositif portable, plus particulièrement il consiste, par exemple, en une carte à puce, une carte sans contact, une carte PCMCIA, un badge, une montre intelligente.

Enfin, le dispositif électronique de l'invention peut être un dispositif extérieur constitué d'une machine ou installation destinée à tester le bon fonctionnement de générateurs aléatoires embarqués à bord desdits dispositifs portables. Ce dispositif extérieur permet un échange d'informations avec le dispositif portable de manière à vérifier que le générateur aléatoire fonctionne correctement. Le dispositif extérieur inter-

agit avec le dispositif portable pour vérifier l'intégrité de son générateur aléatoire.

REVENDICATIONS

1. Procédé de test de source de nombre aléatoire embarqué à bord d'un système cryptographique, du type carte à puce, comprenant les étapes suivantes:

- première étape: génération d'une séquence de (Q+K)*L bits par la source aléatoire, Q, K et L étant des paramètres d'entrée, lesdits bits de la séquence étant groupés par bloc de L bits, formant une séquence d'entiers compris entre 0 et 2^L-1 de longueur Q+K, la longueur étant mémorisée dans le tableau block[n], où n est compris entre 1 et Q+K.
- deuxième étape: calcul du paramètre du test, noté fTU, comprenant les étapes suivantes, appelées sous-étapes, 2.1 à 2.5
  - 2.1 création et initialisation d'un tableau tab [i] de taille 2^L;
  - 2.2 pour n variant de 1 à Q, exécution du calcul: tab[block[n]]=n;
  - 2.3 initialisation du nombre Sum à 0;
  - 2.4 pour n variant de Q+1 à Q+K, exécution du calcul en deux opérations:
    - addition du log(n-tab[block[n]] à Sum;
    - exécution du calcul: tab[block[n]]=n;
  - 2.5 le paramètre fTU du test etant donné par le calcul de la formule:
    fTU=(Sum/K)/Log(2);
- troisième étape: calcul de la variance par block de paramètre du test, notée Var, a partir de l' expression suivante:

$$Var= (1-z)^* \sum_{i=1}^{\infty} \log2(i)^2 * z^{i-1} - ((1-z)^* \sum_{i=1}^{\infty} \log2(i)^* z^{i-1})^2 ,$$

avec $\log2(z)=\log(z)/\log(2)$ et $z=1-2^{-L}$

- quatrième étape: Calcul de la fonction c(L,K);
- cinquième étape: Calcul de l'écart type du paramètre de test, noté σ à partir de la formulation: $\sigma=c(L,K)^*\sqrt{(Var/K)}$;

- sixième étape: calcul du paramètre y; y etant déterminé à partir du taux de rejet du test fixé en entrée, noté ρ, y devant vérifier l'équation: $N(-y)= \rho$.
  N est la fonction de densité normale
- septième étape: calcul de la valeur moyenne idéale du test, notée E[fTU], donnée par la formule suivante.

$$E[fTU]= (1-z)^* \sum_{i=1}^{\infty} \log2(i)^{2*}z^{i-1}$$

avec $\log2(z)=\log(z)/\log(2)$ et $z=1-2^{-L}$

- huitième étape: Calcul des bornes t1 et t2. Elles sont données par l'équation:

  $t1=E[fTU]-y^*\sigma$ et $t2=E[fTU]+y^*\sigma$;

- neuvième étape: résultat du test : le générateur de nombre aléatoire étant accepté si le paramètre du test fTU est compris entre t1 et t2, et rejeté dans le cas contraire,

ledit procédé étant caractérisé en ce que la quatrième étape consiste en un calcul de la fonction c(L,K) valable quelques soient les paramètres L et K.

2. Procédé de test de source de nombre aléatoire selon la revendication 1 caractérisé en ce que la quatrième étape consiste en un calcul de la fonction c(L,K) valable dans le cas où la valeur de L est compris entre 3 et 16 et la valeur de K est supérieur à 30^*2^L.

3. Procédé de test de source de nombre aléatoire selon la revendication 1 caractérisé en ce que la quatrième étape consiste en un calcul de la fonction c(L,K) valable pour une valeur de L>16 et une valeur de $K>30^*2^L$.

4. Procédé selon la revendication 1 caractérisé en ce que le calcul de la fonction c(L,K) comporte neuf étapes:

1. calcul de: $u=1-2^{-L}$ et $v=1-1/(2^L-1)$;

u et v étant des réels;

2. création de deux tableaux tab1 et tab2 de dimension $60*2^L$;
3. remplissage des tab1 et tab2: pour cela,
   3.1 exécution z=u, sum=0, z1=1;
   3.2 pour i variant de 1 à $30*2^L$, répétition des deux opérations étant:
      addition de log2(i)*z1 à sum, dans laquelle log2 désigne le logarithme en base 2, et
      calcul de z1=z1*z;
   3.3 exécution de tab1[0]=(1-z)*sum:
   3.4 pour i variantde 1 à $60*2^L$,
   exécution de tab1[i]=(tab1[i-1]-(1-z)*log2(i))/z
   3.5 répétition les étapes 3.1, 3.2, 3.3, 3.4 en remplaçant u par v et tab1 par tab2;
4. calcul de la variance par bloc notée Var;
   4.1 exécution de sum=0 et x=1;
   4.2 pour i variant de 1 à $30*2^L$, exécution les deux opérations étant:
      addition de $\log2(i)^2*x$ à sum et
      éxécution x=x*z
   4.3 calcul $Var=sum/2^L-tab1[0]^2$;
5. calcul de P(K):
   5.1 calcul de sum=0 et x=1;
   5.2 pour i variant de 1 à $30*2^L$: exécution des trois opérations suivantes:
   calcul de y: $y=u^{2*}(tab2[i+K-1]-tab1[i+K])*(tab2[0]-v^{i*}tab2[i])+u*tab1[0]*(tab1[i+K-1]-tab2[i+K-1])$,
   addition de y*x à sum,
   exécution x=x*u;
   5.3 exécution$P(K)=u^{(K-1)}*sum$;
6. calcul de P(1):
mêmes opérations qu'à l'étape 5 en remplaçant K par 1;
7. calcul de Q(K):
   7.1 exécution de sum=0, sum2=0 et x=1,

7.2 pour i variant de 1 à 30*2^L:
addition de i*log2(i)*$u^{(i-2)}$ à sum2;
exécution les trois opérations suivantes:
calcul de $y=u^{2}$*(tab2[i+K-1]-tab1[i+K])*((i+k)*tab2[0]-v^{i}*tab2[i])-$2^{(-L)}$*sum2)+u*(i+K-1)*tab1[0]*(tab1[i+K-1]-tab2[i+K-1]),
addition de y*x à sum,
exécution de x=x*u;
7.3 exécution de $Q(K)=u^{(K-1)}$*sum
8. calcul de Q(1)
même procédé qu'à l'étape 7 en remplaçant K par 1
9. calcul de c(L,K)
$c(L,K)=\sqrt{(1-2/Var*(P(1)-P(K)-(Q(1)-Q(K))/K)}$

5. Procédé selon la revendication 2 caractérisé en ce que la fonction c(L,K) comporte deux étapes:

Première étape: Lecture des valeurs de e(L) et d(L), e et d étant des réels, listées dans le tableau suivant, pour L compris entre 3 et 16:

L	d(L)	e(L)
3	0, 2732725	0,4890883
4	0,3045101	0,4435381
5	0,3296587	0,4137196
6	0,3489769	0,3941338
7	0,3631815	0,3813210
8	0, 3732189	0,3730195
9	0,3800637	0,3677118
10	0,3845867	0,3643695
11	0,3874942	0,3622979
12	0,3893189	0,3610336
13	0,3904405	0,3602731
14	0,3911178	0,3598216
15	0,3915202	0,3595571

16	0,3917561	0,3594040

Deuxième étape: Calcul de la valeur c(L,K) à l'aide de la formule:

$$c(L,K)=\sqrt{(d(L)+e(L)*2^{L}/K)}$$

6. Procédé selon la revendication 3 caractérisé en ce que le calcul de la fonction c(L,K) est réalisée par la formule suivante:

$$c(L,K)=\sqrt{(1-6/\Pi^{2}+2/\Pi^{2}*(4*\log(2)-1)*2^{L}/K)}$$

7. Dispositif électronique d'auto-vérification d'intégrité physique d'un circuit intégré s'auto-vérifiant et contrôlant l'intégrité de son générateur aléatoire, afin de s'assurer que ce dernier fonctionne correctement en général et ne présente pas de dérive suite à des changements de paramètres externes d'origine malveillante telle qu'une altération par des radiations induites en particulier, caractérisé en ce que ledit dispositif met en oeuvre le procédé de test selon l'une quelconque des revendications 1 à 6.

8. Dispositif électronique selon la revendication 7 caractérisé en ce que le dispositif effectuant le test est un dispositif portable.

9. Dispositif électronique selon la revendication 8 caractérisé en ce que le dispositif est une carte à puce.

10. Dispositif électronique selon la revendication 8 caractérisé en ce que le dispositif est une carte sans contact.

11. Dispositif électronique selon la revendication 8 caractérisé en ce que le dispositif est une carte PCMCIA.

12. Dispositif électronique selon la revendication 8 caractérisé en ce que le dispositif est un badge.

13. Dispositif électronique selon la revendication 8 caractérisé en ce que le dispositif est une montre intelligente.

14. Dispositif électronique selon l'une quelconque des revendications 1 à 6 caractérisé en ce qu'un dispositif extérieur effectuant le test est constitué d'une machine ou installation destinée à tester le bon fonctionnement de générateurs aléatoires embarqués à bord desdits dispositifs portables.